AMENDMENTS TO THE DRAWINGS

The attached sheet of drawings includes changes to Fig. 7. This sheet replaces the original sheet. In Fig. 7, "CONNECT" has been replaced with --CONNECT--.

Attachment: Replacement sheet
Annotated sheet showing changes

REMARKS

Applicants wish to thank the Examiner for the thorough consideration given the present application. Claims 1-50 are presently pending in the present application. Claims 1-5, 7, 8, 10-15, 17, 18, 20, 21, 23, 24, 26, 27, 29, 30, and 32 are amended. Claims 1, 5, 7, 8, 10, 11, 15, 17, 18, 20, 21, 23, 24, 26, 27, 29, 30, 32, and 45-48 are independent claims.

The Examiner is respectfully requested to reconsider the outstanding rejections in view of the above amendments and the following remarks.

Claim for Priority

It is gratefully acknowledged that the Examiner has recognized Applicants' claim for foreign priority. In view of the fact that Applicants' claim for foreign priority has been perfected, no additional action is required from Applicants' at this time.

Specification

The specification has been amended above. Specifically, in order to correct a typographical error, "IV" has been replaced with --IT--. Applicants respectfully submit that no new matter has been added to the application by this amendment.

Drawings

Attached hereto are drawing corrections to Fig. 7. Specifically, in order to correct a typographical error, "CONNET" has been replaced with --CONNECT-- in Fig. 7. Applicants respectfully submit that no new matter has been to the application by this drawing correction.

Acknowledgment of Information Disclosure Statements

The Examiner has acknowledged the Information Disclosure Statements filed on respectively on November 16, 2001, June 18, 2004, and August 18, 2005. Initialed copies of the PTO-1449s have been received from the Examiner. No further action is necessary at this time.

Rejection Under 35 U.S.C. § 102

Claims 1-7, 11-17, 21-23, 27-29, 33, 35, 37, 39, and 41-44 stand rejected under 35 USC § 102(e) as being anticipated by U.S. Patent No. 5,796,836 to Markham (hereafter "Markham"). This rejection, insofar as it pertains to the presently patented claims, is respectfully traversed.

In Markham, the encryption of one plain text block is **decoupled** from the encryption of the next plain text box, even if both blocks are parts of the same plain text data. Specifically, Markham teaches that the encryption of each plain text block is performed using a pseudorandom vector.

In order to decouple encryption of successive plain text blocks, Markham teaches that a plurality of pseudorandom vectors are pre-computed. For instance, assuming that two pre-computed pseudorandom vectors (IV_1 and IV_2) are being used, Markham teaches that the first pre-computed vector (IV_1) is used for encrypting the first block of plain text (M_1), while the second pre-computed vector (IV_2) is used for encrypting the second block of plain text (M_2). Thereafter, Markham teaches that the keystream generated by encrypting the first plain text block (M_1) is used to encrypt the third plain text block (M_3), while the keystream generated by encrypting the second plain text block (M_2) is used for encrypting the fourth plain text block (M_4). Similarly, in Markham, the results of encrypting M_3 is used to encrypt M_5, etc., while the results of encrypting M_4 is used to encrypt M_6, etc.

Thus, Markham teaches a plurality of encrypting processes corresponding to the number of pre-computed pseudorandom vectors. In other words, in the above example where two pre-computed vectors are used, Markham's system employs a first encrypting process for encrypting

plain text blocks M_1, M_3, M_5, etc., and a second encrypting process for encrypting M_2, M_4, M_6, etc. Accordingly, none of Markham's encrypting processes encrypts a logically continuous set of data elements, such as a successive set of plain text data blocks (M_1, N_2, N_3...). Also, because Markham similarly discloses decoupling the decryption of one cipher block from the next cipher block, each decrypting process in Markham fails to produce a continuous set of data elements (e.g., plain text blocks).

As amended, independent claim 1 recites an encrypting process of first processing data, which "comprises a first logically continuous set of data elements." Claim 1 further recites starting an encrypting process of a second processing data before completing the encrypting process of the first processing data. Independent claims 5, 7, 21, and 23 also recite similar features, as amended.

Also, independent claim 11 has been amended to recite a decrypting process of first processing data, which "comprises a first logically continuous set of data elements when decrypted." Claim 11 further recites starting a decrypting process of a second processing data before completing the decrypting process of the first processing data. Independent claims 15, 17, 27, and 29 also recite similar features, as amended.

Applicants respectfully submit that Markham fails to disclose these claimed features. As described above, Markham decouples the encrypting and decrypting of each block from the next block. Thus, none of the encrypting processes in Markham encrypts a logically continuous set of data elements. Similarly, none of Markham's decrypting processes generates a logically continuous set of data elements.

At least for the reasons set forth above, Applicants respectfully submit that claims 1, 5, 7, 11, 15, 17, 21, 23, 27, and 29 are allowable. Accordingly, Applicants submit that claims 2-4, 6, 12-14, 16, 22, 28, 33, 35, 37, 39, and 41-44 are allowable at least by virtue of their dependency on an allowable independent claim. Therefore, the Examiner is respectfully requested to reconsider and with this rejection.

Claims 45-50 stand rejected und 35 U.S.C. § 102(e) as being anticipated U.S. Patent No. 6,226,742 to Jakubowski et al. (hereafter Jakubowski). This rejection is respectfully traversed.

Independent claims 45 and 46 each recite "a message authentication code (MAC) generator for inputting the [encrypted/decrypted] data output from the [encrypting/decrypting] unit and generating a MAC for insuring of integrity of the encrypted data." Similarly, independent claims 47 and 48 recite "a MAC generating step for encrypting the [encrypted/decrypted] data output from the [encrypting/decrypting] step and generating a MAC for ensuring an integrity of the encrypted data."

The Examiner cites col. 9, lines 4-33 in Jakubowski to provide a teaching of the aforementioned features (see Office Action at pgs. 10-11). This section of Jakubowski describes the encrypting processing illustrated in Fig. 4A. In the cited passage, Jakubowski discloses that the encryption process includes the following steps: starter block

> "generating, in response to an incoming plaintext message, an intermediate stream, wherein **a predefined portion of the intermediate stream defines a message authentication code** (MAC); inserting an encrypted version of the MAC into a predefined portion of a cipher text message; and generating, in response to the intermediate stream and the encrypted MAC, a remainder of the cipher text message such that the remainder exhibits a predefined variation...also contained within the encrypted MAC." (col. 9, lines 6-16; emphasis added)

Jakubowski further discloses that the decryption process (Fig. 4B) proceeds in "essentially a reverse fashion to that of encryption" (col. 9, lines 16-17).

Accordingly, Applicants respectfully submit that Jakubowski fails to disclose a MAC generating unit or method, which inputs encrypted/decrypted data output from an encrypting/decrypting unit. Instead, Jakubowski expressly teaches that the MAC is generated from the **intermediate stream**. During encryption, this intermediate stream is produced before encrypted data (ciphertext) is output from the encrypting unit/step. Likewise, during decryption,

the intermediate stream is recovered before plaintext data is output from the decrypting unit/step. Thus, Applicants respectfully submit that Jakubowski fails to teach or suggest every claimed feature in claims 45-48.

At least for the reasons set forth above, Applicants respectfully submit that claims 45-48 are allowable. Accordingly, Applicants submit that claims 49 and 50 are allowable at least by virtue of their dependency on claims 47 and 48. Thus, the Examiner is respectfully requested to reconsider and withdraw this rejection.

Rejection Under 35 U.S.C. § 103

Claims 8-10, 18-20, 24-26, 30-32, 34, 36, 38, and 40 stand rejected under 35 USC § 103(a) as being unpatentable over Markham in view of Jakubowski. This rejection is respectfully traversed.

Independent claims 8, 10, 24, and 26 recite that ciphertext block data C_i, which is identical to the ciphertext block data C_i output from the encrypting unit/step, is input to the MAC generator/generating step.

In the rejection, the Examiner relies on Jakubowski to teach the claimed MAC generator/generating step (see, e.g., page 12 of the Office Action). The Examiner cites sections of Jakubowski, which describe the encryption and decryption processes of Figs. 4A and 4B, respectively.

However, according to Fig. 4A and col. 9, lines 6-16 (quoted above), Jakubowski's MAC is defined as a predetermined portion of the intermediate stream $Y_0 \ldots Y_n$, which is encrypted and inserted into the output ciphertext $C_0 \ldots C_n$. Thus, as shown in Fig. 4A, Jakubowski fails to teach that a ciphertext block C_i is used as an input for generating the MAC, as required by claims 8, 10, 24, and 26.

As amended, independent claims 18, 20, 30, and 32 now recite that "the ciphertext block data C_i is input to the MAC [generator/generating step] before the ciphertext block data C_{i+1} is decrypted by the decrypting [unit/step]," or a feature similar thereto.

Also, Jakubowski's decryption process of Fig. 4B shows the ciphertext $C_0 \ldots C_n$ being deciphered to generate the intermediate stream $Y_0 \ldots Y_n$. Thereafter, Fig. 4B shows that the intermediate stream is fully generated, the MAC is recovered by applying a cipher block chain (CBC) on the intermediate stream to recover the plaintext message, and then applying a CBC on the resulting plaintext message to recover the MAC. This process is discussed in col. 10, lines 14-17, which states:

> "...after the plaintext message has been recovered, that particular plaintext message is then processed through a backward CBC to generate a recreated (recovered) MAC."

Thus, Jakubowski's decryption process generates the MAC by applying CBC on the **plaintext message** -- not the ciphertext. Therefore, Jakubowski fails to disclose inputting a ciphertext block data C_i to the MAC generator or generating step before the ciphertext block data C_{i+1} is decrypted, as required by claims 18, 20, 30, and 32.

Applicant respectfully submits that independent claims 8, 10, 18, 20, 24, 26, 30, and 32 are allowable at least for the reasons set forth above. Accordingly, Applicants submit that claims 9, 19, 25, 28, 31, 34, 36, 38, and 40 are allowable at least by virtue of their dependency on allowable independent claims. Therefore, the Examiner is respectfully requested to reconsider and withdraw this rejection.

Conclusion

Should the Examiner believe that any outstanding matters remain in the present application, the Examiner is respectfully requested to contact Jason W. Rhodes (Reg. No. 47,305) at the telephone number of the undersigned to discuss the present application in an effort to expedite prosecution.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Dated: December 30, 2005

Respectfully submitted,

By _____
D. Richard Anderson
Registration No.: 40,439
BIRCH, STEWART, KOLASCH & BIRCH, LLP
8110 Gatehouse Road
Suite 100 East
P.O. Box 747
Falls Church, Virginia 22040-0747
(703) 205-8000
Attorney for Applicant

Attachments